Board of Governors of the Federal Reserve System

AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

September 2004

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

September 30, 2004

The Honorable Mark W. Olson
Chairman, Committee on Board Affairs
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Governor Olson:

The Office of Inspector General is pleased to present its *Report on the Audit of the Board's Information Security Program*. We performed this audit pursuant to requirements in the Federal Information Security Management Act (FISMA), which requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices. This was the fourth year that such evaluations were required. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate compliance by the Board of Governors of the Federal Reserve System (Board) with FISMA and related information security policies, procedures, standards, and guidelines.

To test security controls and techniques, we reviewed controls over the Board's database application (DB2) and three applications that interface with that software. We also reviewed security settings for selected hardware such as servers, workstations, and routers. Our review of DB2 and our security control tests of the applications did not identify any significant security control deficiencies, although we found several areas where controls need to be strengthened. Our review of security settings also identified additional improvement opportunities related to documentation and the processes for establishing, monitoring, and remediating security settings. Given the sensitivity of the issues involved with these reviews, we are providing the specific results to management under separate restricted cover.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations in our 2003 information security audit report and reviewed the Board's processes related to security control reviews, certifications and accreditation, remedial action monitoring, incident response, security awareness and training, and patch management.[1] Our follow-up work showed that over the past year the Board has

[1] See our *Report on the Audit of the Board's Information Security Program* (A0302), dated September 2003.

continued to make progress in developing and implementing a structured information security program as outlined by FISMA and the actions taken are sufficient to allow us to close all of our previous recommendations. We did find, however, that opportunities exist to further enhance the Board's information security program and strengthen compliance with the legislative requirements and related guidance. Our report contains five recommendations designed to improve the Board's procedures related to the plan of action and milestones, security training, security reviews, system inventory, and incident response.

In addition, based on our review of recent security-related guidance produced by the National Institute of Standards and Technology and the Office of Management and Budget (OMB), we believe that over the coming year the Board will need to fundamentally redesign many of its information security processes to remain consistent with applicable standards. These changes will affect the Board's current processes for risk assessments, control identification and review, as well as certification and accreditation. While we do not have any specific recommendations at this time, the final section of our report discusses several significant challenges for Board management as they begin implementing these new standards and guidelines. Because complying with these new requirements will, in our opinion, be essential to maintaining compliance with the security legislation, Board management will need to make the necessary time and resource commitment to ensure that this transition is completed effectively and timely.

We provided our draft report to the director of the Division of Information Technology, who serves as the Board's Chief Information Officer for FISMA purposes, for review and comment. In her response, the director concurred with our recommendations regarding enhancements to the Board's plan of action and milestones, security training, and security review procedures and her response describes actions that have been or will be taken to address these recommendations. The director also agreed with our recommendation that the inventory of applications and general support systems should include the identification of interfaces as required by FISMA, but she did not agree that further coordination of system classifications for FISMA and other reporting purposes was necessary. We continue to believe that applications which have been designated as mission critical for contingency planning or critical infrastructure protection purposes require a level of attention under FISMA greater than bundling them under the Board's general support system. Regarding our recommendation to expand reporting of security incidents, the director agreed that the Board's reporting to the appropriate government agencies should include incidents that occur at the Reserve Banks and other third-party contractors, but only when they have a material impact on Board operations. The director does not agree, however, that expanding the Board's reporting of unsuccessful penetration attempts is useful, given the resources required to collect and report the additional statistics. The director also expects the current reporting guidance regarding unsuccessful attempts to be revised. We continue to believe that the Board needs to realign its reporting procedures with current reporting requirements; however, we are encouraged by its proactive efforts to identify additional methods of security incident detection. We will also monitor efforts to update collection and reporting guidance and we will review the Board's processes in light of any changes.

We are providing copies of this audit report to Board management officials. In addition, the Chairman will provide the report to the director of OMB as required by FISMA. The report will be added to our publicly available web site and will be summarized in our next semiannual report to the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

/signed/

Barry R. Snyder
Inspector General

Enclosure

cc: Governor Edward M. Gramlich
Governor Donald L. Kohn
Mr. Stephen Malphrus
Ms. Marianne Emerson

Board of Governors of the Federal Reserve System

AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

September 2004

TABLE OF CONTENTS

Page

BACKGROUND

Legislative Requirements

The Federal Information Security Management Act of 2002 (FISMA), Title III of Public Law 107–347, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA requires that each agency develop and implement an agencywide security program to provide information security throughout the life cycle of all agency systems, including systems managed on behalf of the agency by another agency, contractor, or other source. The agency's program should include

- conducting periodic risk assessments;
- developing security plans;
- establishing minimum security configuration requirements;
- providing security awareness training;
- conducting periodic control testing;
- establishing procedures for detecting, reporting, and responding to security incidents; and
- developing a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies.

FISMA looks to the agency's Chief Information Officer (CIO) to ensure compliance with the act's requirements.

FISMA also requires each agency Inspector General (IG) to perform an annual independent evaluation of their agency's information security program and practices. The evaluations are designed to test the effectiveness of controls and techniques for a representative subset of the agency's information systems and to assess compliance with the requirements of FISMA. Each agency head is required to submit the results of the IG's independent evaluation, along with the agency's reports of the adequacy and effectiveness of information security policies, procedures, and practices, to the director of the Office of Management and Budget (OMB) on an annual basis.

FISMA assigned to the director of OMB the responsibility for establishing governmentwide policies for the management of information security programs. FISMA also tasked the National Institute of Standards and Technology (NIST) with developing standards and guidelines related to categorizing information and information systems; recommending the types of information and information systems to be included in each category; establishing minimum security requirements for information and information systems; and detecting and handling security incidents. To assist agencies in fulfilling their FISMA evaluation and reporting responsibilities, OMB issued memorandum M-04-25 in August 2004. Consistent with prior years' guidance, the memorandum emphasizes reporting based on security-related performance measures, although this year's guidance contains more detailed performance measures regarding security configuration management and security incident procedures. The guidance also asks each Office

of Inspector General (OIG) to assess their agency's plan of action and milestones (POA&M) process as well as their agency's certification and accreditation process.

Information Security Roles and Responsibilities

The Board of Governors of the Federal Reserve System (Board) has designated the Staff Director for Management as the Board's CIO. The Staff Director has delegated to the director of the Division of Information Technology (IT) certain CIO functions pertaining to FISMA and E-Government. An IT assistant director serves as the Board's Information Security Officer (ISO) and is the focal point for the Board's information security activities. The ISO is responsible for the Board's Information Security Unit. The unit's responsibilities include administering the Board's information security program; monitoring the Board's security posture; and intervening, as required, to address security exposures and incidents. Appendix 1 contains an organizational chart depicting these functions.

Because much of the information technology at the Board is decentralized, divisions and offices also have information security responsibilities, including performing risk assessments and ensuring proper security controls are in place. To help coordinate these responsibilities, the Board has established an Information Security Committee (ISC) comprised of representatives from each division and office. The ISC functions as a Boardwide coordinating body with responsibility for advising management regarding information security strategic direction and initiatives.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted our audit fieldwork from April through September 2004. Our audit objectives, based on FISMA's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate the Board's compliance with FISMA and related information security policies, procedures, standards, and guidelines. To achieve our objectives, we reviewed Board and Federal Reserve System (System) documentation pertaining to information security and met with officers and staff with information security responsibilities throughout the Board. We reviewed five security control reviews performed during the past year by independent Board consultants as well as the process for conducting control reviews internally by Board staff in divisions other than IT. We also reviewed the Board's processes related to certifications and accreditation, remedial action monitoring, incident response, security awareness and training, and patch management.

To test security controls and techniques, we reviewed controls over the Board's database application (DB2) and selected three applications for review and evaluation that interface with DB2. We performed our application control tests using a modified version of NIST Special Publication 800-26*, Security Self-Assessment Guide for Information Technology Systems*. We also reviewed security settings for selected hardware such as servers, workstations, and routers. In addition, we followed up on open issues from prior control reviews.

To evaluate the Board's compliance with FISMA, we followed up on the status of the recommendations made in our prior independent evaluation of the Board's information security program and practices.[2] We also compiled information on those areas for which OMB requested a specific response as part of the agency's annual FISMA reporting; our response will be provided to OMB under separate cover. Although we obtained information related to processes for implementing FISMA's requirements for systems included in the Board's inventory but maintained by the Reserve Banks, we did not perform any testing of these processes or conduct any control testing related to these systems. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, we found that the Board's information security practices remain generally effective. Our review of DB2, our security control tests of three applications, and our follow-up work of the recommendations on prior control tests did not identify any significant deficiencies. We did, however, find several areas where controls could be strengthened. Our work related to OMB's questions regarding configuration management also identified additional improvement opportunities related to documentation and the processes for establishing, monitoring, and remediating security settings. Given the sensitivity of the issues involved, we are providing the results to management under separate restricted covers and we plan to follow up on our recommendations as part of our future information security audit activities. Our follow-up work on prior control tests allowed us to close all outstanding recommendations.

We also found that over the past year the Board has continued to make progress in developing and implementing a structured information security program as outlined by FISMA. Specifically, the Staff Director for Management delegated the CIO function to the director of IT for FISMA and selected E-Government functions. The delegation establishes a more direct reporting relationship between the CIO and ISO for FISMA purposes. In addition, IT created and staffed a new analyst position reporting to the ISO. The analyst's responsibilities include performing security reviews; the use of contractors has been phased out and all security reviews will be performed internally. The ISO has also finalized the Boardwide security plan, updated the Board's inventory to include third-party applications maintained on behalf of the Board by contractors and Reserve Banks, implemented additional methods to provide security awareness and training, and established a process for updating the Board's POA&M. These actions are sufficient to allow us to close all recommendations from our previous independent evaluation.

Notwithstanding these actions, we believe the Board's POA&M, security training, security reviews, system inventory, and incident response procedures could be improved to enhance the Board's information security program and strengthen compliance with the legislative requirements and related guidance. Our report contains five recommendations designed to address these areas. In addition, based on our review of recent guidance produced by NIST and

[2] See our *Report on the Audit of the Board's Information Security Program* (A0302), dated September 2003.

OMB, we believe that over the coming year the Board will need to fundamentally redesign many of its information security processes to remain consistent with applicable standards. These changes will affect the Board's current processes for risk assessments, control identification and review, as well as certification and accreditation. While we do not have any specific recommendations at this time, the final section of our report discusses several significant challenges for the CIO, ISO, and program officials as they begin implementing these new standards and guidelines.

1. **We recommend that the CIO enhance the process for prioritizing, tracking, and managing security performance gaps by (1) providing additional guidance on the level of detail that should be reported on POA&Ms and (2) ensuring that all security-related tasks are monitored through the Board's POA&M process.**

FISMA requires agencies to establish a process for addressing any deficiencies in information security policies, procedures, and practices. To implement this requirement, OMB has issued guidance requiring agencies to prepare and submit POA&Ms for all programs and systems where an information technology security weakness has been found. The guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control. The plans should include all security weaknesses found during any review done by, for, or on behalf of the agency, including Government Accountability Office audits, financial statement audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agencywide management tool for identifying the specific tasks required to address identified weaknesses, as well as the associated resources and anticipated milestones. In addition, program officials should regularly update the CIO on their progress in implementing corrective actions to enable the CIO to monitor agencywide remediation efforts and provide the agency's quarterly update to OMB.

During last year's audit, we found that the ISO had not issued specific guidance to divisions and offices as to what information should be tracked at the division level. Since then, the ISO has reviewed the process for updating the Board's POA&M and issued guidance to the divisions that includes basic reporting requirements. All divisions and offices now prepare and submit a POA&M to the ISO on a quarterly basis. This provides the foundation for helping the ISO identify potential trends and developing a reference tool for identifying corrective actions should similar issues occur elsewhere at the Board. As a result of these actions, we closed our previous recommendation.

We believe, however, that the Board's POA&M process can be further enhanced by providing additional guidance expanding the level of detail required on the divisions' POA&Ms. During this year's audit, we found that the information provided by the divisions was insufficient to ensure that all weaknesses had been identified, were properly tracked, and were corrected in accordance with established milestones. For example, we found that several POA&Ms only noted that a control review had been conducted; there was no information regarding weaknesses found during the review, the required corrective actions, or the expected level of effort. Without this level of detail, program officials cannot use the POA&Ms to effectively monitor their division's actions for correcting information security weaknesses and the ISO has insufficient information to effectively identify issues with Boardwide implications. The CIO should expand

current guidance to firmly establish the expected level of detail to be provided by the divisions. As guidance is developed, the CIO will also need to ensure that the guidance is provided to Reserve Bank staff who will be conducting reviews on applications maintained in support of the Board's supervision and regulation function. This will help ensure that weaknesses related to all applications on the Board's inventory are tracked in a consistent manner.

We believe the Board's current process can also be improved by ensuring that the Board's overall POA&M includes security weaknesses and issues identified at the division level and by expanding the sources of information used to identify security-related issues. During our audit, we found that weaknesses and corrective actions in the divisions' POA&Ms—when the weaknesses and actions were identified—are not included in the Board's overall POA&M. In our opinion, some of the division-level tasks identify security improvements with Boardwide implications such as patch management, remote access, password integrity, and encryption. We believe the ISO should also track these issues from an agency-level perspective. In addition, we found that weaknesses identified on reviews other than FISMA-related control reviews or other information security efforts, such as penetration tests and vulnerability scanning, are not included in the Board's POA&M. For example, the OIG recently completed an evaluation of the Board's emergency preparedness initiatives and identified several security-related actions for management's attention. Similarly, the Board's recent submission to OMB as required by *Homeland Security Presidential Directive – 7* (HSPD-7) identified ongoing and planned tasks related to critical infrastructure protection.[3] None of the issues identified in these reports were included in the Board-level POA&M, although one issue was partially addressed in a division POA&M. While we recognize that these tasks may be tracked by Board staff through other mechanisms and that many of the issues may pertain more directly to physical security matters, we believe the reports have information security ramifications and should be incorporated into the Board's POA&M. Since the ISO may not routinely be included in all audit and other review report processes, the CIO will need to develop guidance to establish the required level of Boardwide coordination to ensure that security-related issues are centrally and consistently monitored.

2. We recommend the CIO establish a process to develop feedback on the effectiveness of the Board's security awareness and training program.

FISMA tasks the head of each agency with ensuring that the agency has trained personnel sufficient to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. Specifically, FISMA requires an agency's information security program to include security awareness training to inform all personnel, including contractors and other users of information systems that support the agency's operations and assets, of the

[3] *Homeland Security Presidential Directive – 7*, issued in December 2003, states that all federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. The directive notes that, consistent with FISMA, agencies are to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. The directive also required all federal departments and agencies to develop and submit to OMB plans for protecting the physical and cyber critical infrastructure and key resources that the agencies own and operate. Although the Board did not believe it was fully subject to OMB's reporting instructions, the Board submitted the required information.

information security risks associated with their activities as well as their responsibilities in complying with agency policies and procedures. FISMA also requires that the CIO train and oversee personnel with significant responsibilities for information security.

The Board's security awareness program includes several components. Information security staff periodically post security awareness articles and "tip sheets" on the Board's internal website. During the past year, these articles have covered topics such as viruses, remote access, and computer hacking. Information security staff have also conducted three lunchtime technology seminars. In addition, new staff members receive an introduction to the Board's information security program during new employee orientation, and all staff, including contractors, are required to complete an annual security awareness test. To help meet its requirement for training individuals with significant security responsibilities, the Board contracted with an information technology training company to provide web-enabled security training. Because responsibility for identifying employees with significant security responsibilities and for selecting the appropriate training rests with the individual divisions and offices, individual training programs may include courses other than the web-based training provided by the contractor. The actions taken during the past year address our previous recommendation to establish additional proactive training measures.

Although the Board has established an acceptable security awareness and training program in compliance with FISMA requirements, we believe the program can be enhanced by developing and implementing a monitoring and feedback process to ensure the program is working as intended. As noted in NIST guidance on building an information technology security awareness and training program, continuous improvement should always be the theme for security awareness and training initiatives. Once a program has been implemented, processes must be put into place to monitor compliance and effectiveness. Formal evaluation and feedback mechanisms are critical components of any education program.

We believe there are several ways for the Board to establish feedback mechanisms. This year's security awareness test, for example, included questions related to the security articles written during the year. However, the test was not monitored to identify how many employees correctly answered each of the questions. We believe this type of feedback could help determine whether the articles were effectively presented. If a particular question was answered incorrectly by a majority of the employees, the topic would be a candidate for a future awareness article, tip sheet, or seminar. We also believe that as Board staff with significant security responsibilities complete their training programs, there should be a mechanism to provide the ISO with feedback on the effectiveness of the material, particularly for the recently contracted web-based training. A feedback mechanism would provide the ISO with information to fine tune training requirements, add or delete material, and modify the implementation method as required. The feedback might also identify courses which could become baseline requirements for all individuals with particular security responsibilities (e.g., network administrators or application developers). Information on courses outside the web-based instruction would help the ISO identify additional training opportunities that might be useful on a Boardwide basis.

3. We recommend that the CIO provide guidance for conducting information security reviews that (1) includes specific requirements for control testing and (2) establishes greater consistency across all reviews.

FISMA requires periodic testing and evaluation of the effectiveness of an agency's information security policies, procedures, and practices. The evaluation is to include testing of the management, operational, and technical controls for every system identified in the agency's inventory and is to be performed with a frequency depending on risk, but not less than annually. The depth and breadth of these annual reviews depends on the potential risk and magnitude of harm as well as the relative comprehensiveness of the prior year's review and the adequacy and successful implementation of the POA&M for weaknesses in the system. FISMA looks to NIST to develop the standards and guidelines necessary to assist agency officials in fulfilling this responsibility.

During last year's audit, we noted that while several divisions performed the reviews in-house, IT had relied primarily on outside consultants to perform reviews of the applications that IT maintained. We were concerned that the limited documentation provided by the consultants as part of their reviews could hinder the effective implementation of corrective actions and preclude the retention by Board staff of knowledge gained during the reviews. Since our previous audit, the ISO has hired an analyst whose responsibilities include performing security reviews. The use of contractors has been phased out and all FISMA reviews will now be performed internally.

As part of this year's audit, we performed a more in-depth review of the supporting documentation for five control reviews performed during the past year by the consultants. We also reviewed the process for conducting control reviews internally by Board staff in divisions other than IT. Our review showed that although the consultants had used the NIST self-assessment guide as required by OMB, the reviews did not include detailed testing of technical controls. Rather, the consultant relied primarily on reviewing system documentation and interviewing system owners and technical support staff. While this may provide a level of assurance that the systems have appropriate documentation (e.g., security plans and risk certifications) and that responsible staff understand information security policies, procedures, and practices, it does not ensure all security controls are functioning as intended. For the reviews conducted internally, we found an inconsistent level of reporting or retention of supporting documentation. For example, staff performing the reviews in one division did not document the steps performed or produce a report at the completion of the control review. Instead, they simply made notes on any security weaknesses identified and then held the reviews open until any issues identified were resolved. Although the process outlined by these individuals was consistent with OMB and NIST requirements, without adequate supporting documentation the CIO and ISO have no assurance that the reviews are properly or consistently conducted. In our opinion, holding a review open until all issues are resolved precludes the division from providing timely feedback to the ISO. The lack of a formal report—identifying weaknesses found and corrective actions taken—also reduces the ISO's ability to effectively identify security issues on a Boardwide basis and minimizes the effectiveness of the POA&M process for tracking and prioritizing corrective actions.

4. We recommend that the CIO (1) expand the inventory of applications and systems to include the identification of the interfaces between each system and (2) coordinate the reporting of applications for FISMA purposes with other reporting responsibilities.

FISMA requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. The inventory forms the basis of FISMA's periodic testing requirement and is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency. The inventory should also identify system criticality and risk levels. OMB expects agencies to have an inventory based on work completed in developing an enterprise architecture.

The Board's inventory contains 145 applications and systems, including major applications, general support systems (GSS), and non-major applications with varying degrees of security requirements. Consistent with our previous recommendation, the Board's ISO has worked with the ISC representatives to refine and update the inventory for Board-maintained applications, including making adjustments as to which systems are considered major and non-major. The ISO has also expanded the inventory to include third-party systems maintained by contractors as well as systems maintained by the Reserve Banks in support of the Board's delegated supervision and regulation function.

We found, however, that the Board's inventory does not include the interfaces between each system and all other systems or networks. While we recognize that this information may be contained in other security-related documents such as application security plans, we believe that this information should be consolidated on the Board's application inventory. Consolidation is needed not only to achieve compliance with FISMA and OMB requirements, but also to facilitate upcoming changes to the Board's risk assessment and certification processes. The Board's current risk assessment process is based on assessing risk by business function. Going forward, however, compliance with NIST guidelines will require application-specific risk assessments. In our opinion, identifying the interfaces between all systems will be essential to accurately completing these assessments. Accurately identifying the interfaces is also necessary for completing system certifications and accreditations. The NIST *Guide for the Security Certification and Accreditation of Federal Information Systems*, which is effective for all new systems going into production after May 2004, requires information system owners to confirm during the certification and accreditation process that potential threats which could exploit information system flaws or weaknesses have been properly identified and documented in the system security plan, risk assessment, or equivalent document. The guidance recognizes that system interconnections, if not appropriately protected, may result in compromises of all connected systems and the data they store, process, or transmit.

Our review of the Board's inventory also found that not all applications listed as "critical assets" for either critical infrastructure protection or contingency planning purposes were classified as major applications on the FISMA inventory. For example, one application listed on the Board's HSPD-7 submission as a mission-critical asset is classified as "other" in the Board's inventory; the "other" classification means the application has no security requirements beyond those provided by its GSS. The Board does not require these applications to have separate security

plans or to undergo security control testing beyond what is performed for the GSS. Similarly, we found applications designated in divisions' continuity of operations plans (COOPs) as critical assets for contingency recovery purposes that are classified as "other" applications for FISMA reporting purposes. We recognize that the definition of a system's criticality varies depending on the controlling law or implementing guidance. We believe, however, that there needs to be a rationalization and harmonization between the Board's FISMA inventory, its critical infrastructure protection plan, and the divisions' contingency plans to accurately comply with the OMB requirement of appropriately identifying system criticality and risk levels. Establishing the appropriate designation for FISMA inventory purposes also helps ensure the system undergoes a level of review and testing commensurate with its importance to the Board's primary mission areas. This effort will require the coordination of staffs in IT and the Office of the Staff Director for Management since the latter has overall responsibility for COOP and critical infrastructure protection.

5. We recommend the CIO expand the Board's reporting of security incidents to include all four incident priority levels as well as incidents that occur at the Reserve Banks and other third-party contractors.

FISMA requires agencies to develop procedures for detecting, reporting, and responding to security incidents. The procedures should include mitigating risks associated with such incidents before substantial damage is done; notifying and consulting with the Federal Computer Incident Response Center (FedCIRC)/United States Computer Emergency Readiness Team (US-CERT); and notifying and consulting with appropriate law enforcement agencies and relevant OIGs. FedCIRC/US-CERT defines an incident as an event violating an explicit or implied security policy. These incidents include, but are not necessarily limited to, attempts (either failed or successful) to gain unauthorized access to a system or data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

FedCIRC/US-CERT has also established requirements for incident reporting. As shown in table 1, FedCIRC/US-CERT has established priority levels for categories of incidents and the timeframe under which each priority level should be reported.

Table 1. FedCIRC/US-CERT Priority Levels for Incident Reporting

Priority Level	Description	Examples of Incidents	Timeframe to Report
1	Possible life-threatening activity or affects classified or critical systems or information.	• Root Compromise • User Compromise • Denial of Service • Web-site defacements • Detection of malicious logic	Immediately
2	Incident could become public; provide unauthorized access to network and/or unclassified, non-critical information; affect systems resources; or shows active targeting of classified/critical systems.	• User Compromise • Successful virus/worm infection • Successful introduction of a virus/worm into a network • Scanning of classified or critical systems	Within two hours of discovery/ detection
3	Incident shows active targeting of unclassified, non-critical systems or potential threat to network.	• Scanning of unclassified, non-critical systems • Detection and elimination of malicious logic before infestation	Weekly
4	Incident shows possible malicious intent or unintentional violation of security policy.	• Misuse of resources • Spam e-mail • Fraudulent e-mail • Social engineering	Monthly

The Board has developed an incident reporting process that includes procedures for escalating incident reporting within the Board as well as for reporting to the appropriate government agencies, law enforcement agencies, and the OIG. We found, however, that the Board is only tracking and reporting priority level 1 and 2 incidents. The Board's ISO told us that the Board's process is based on NIST's guidance which provides a narrower definition of an incident than FedCIRC/US-CERT. NIST states an incident can be thought of as a violation or imminent threat of a violation. An imminent threat of a violation refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. Examples include denial of service, malicious code, unauthorized access, and inappropriate usage. Based on the Board's process, the Board only reported three security incidents during the past year.

We understand the magnitude of tracking all levels of incidents, given that thousands or millions of possible signs of incidents may occur each day. We also found that there is an inconsistency among federal agencies in their reporting. However, OMB has stated they expect all incidents to be tracked and reported, and we believe that incorporating priority levels 3 and 4 into the Board's reporting process is necessary to be in compliance with current reporting requirements.

Although FISMA tasks NIST to provide definitions and guidance on identifying and handling security incidents, the reporting requirements are presently established by FedCIRC/US-CERT.

Beyond fulfilling a reporting requirement, however, we also believe that the data could be used for other internal purposes. For example, NIST guidance on detecting and handling security incidents discusses using the data collected for developing lessons learned. The publication suggests that a study of incident characteristics and changes in incident trends could indicate systemic threats or security weaknesses. The data can thus be used in a preventive manner to help identify enhancements to an organization's security measures.

Based on our review of the Board's incident response process, we also believe the CIO needs to develop a mechanism for coordinating incident reporting with contractors or other third parties, especially for any systems where the Reserve Banks are acting as the Board's contractors or processing information on behalf of the Board. FISMA's requirement for reporting and responding to security incidents is part of an agency's overall information security program and the program should apply to all operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. We believe that any incident occurring at the Reserve Banks which affects a Board system or a system processing Board information should be reported and tracked as part of the Board's incident response procedures. Although the Board's ISO may already be notified of incidents occurring at the Reserve Banks, the current notification process will need to be formalized to ensure that timeframes for reporting to the appropriate agencies can be met. The ISO will also need to develop incident reporting procedures for other contractors.

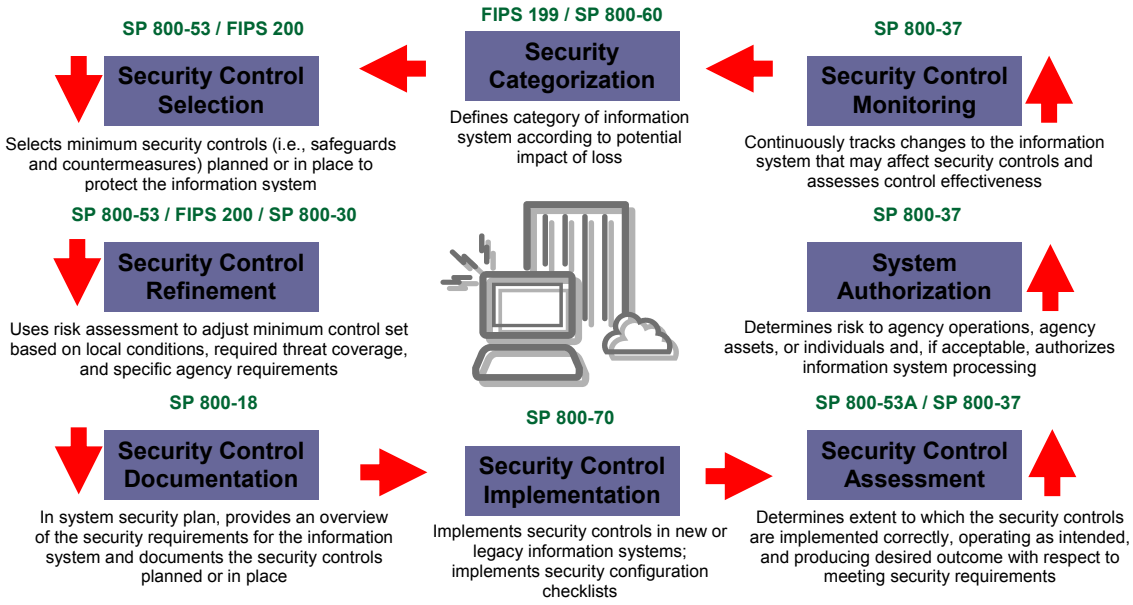
FUTURE CHALLENGES

FISMA tasked NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. To address FISMA's requirements, NIST has issued or is in the process of issuing several federal information processing standards (FIPS) and special publications. FIPS must be implemented as written; the only flexibility exists within the standard itself. Special publications (SP) are considered guidance and allow for agency discretion in guidance implementation.

The NIST guidance issued to date and the draft guidance expected to be finalized over the next year represent, in our opinion, fundamental changes from current Board and System processes with respect to information security management. Implementing this guidance will present the Board with significant challenges in transitioning from its existing policies and procedures. Complying with these new requirements, however, will be essential to maintaining compliance with the security legislation and will likely form the basis of future OIG audit work related to information security. Board management will therefore need to make the time and resource commitment to ensure this transition is completed effectively and timely. Listed below are the

major process changes we believe the Board must make over the coming year and the NIST guidance associated with each process. Figure 1 also depicts the entire risk management framework as envisioned by NIST.

Figure 1. NIST Risk Management Framework



Categorizing and Mapping Information and Information Systems

In December 2003, NIST issued FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 sets the standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, issued in July 2004, provides guidelines recommending the types of information and information systems to be included in each security category.

The Board currently performs risk assessments on a business function (often division-level) basis. Board staff use guidance in the Federal Reserve System's *Information Security Manual* (ISM) to categorize risks (monetary loss, productivity loss, and embarrassment) and vulnerabilities (personnel, facilities and equipment, applications, communications, and environmental software and operating systems).[4] Going forward, risk assessments must be done on an asset-by-asset basis using the guidance in FIPS 199 and SP 800-60. Using this guidance, the Board will need to analyze the threats to and vulnerabilities of information systems and the

[4] To provide policy direction regarding the protection of its information assets, the System developed the Information Security Manual (ISM). The ISM defines policies and safeguards for information security and is applicable to all automated platforms and manual information processes used throughout the System.

potential impact or magnitude of harm resulting from unauthorized disclosure (confidentiality), modification (integrity), or the loss of availability of information and information systems.

Identifying Minimum Security Controls

Currently in draft, publication SP 800-53*, Recommended Security Controls for Federal Information Systems,* provides interim guidance regarding the minimum information security requirements for information and information systems in each category identified in FIPS 199. SP 800-53 will be effective until completion and adoption of FIPS 200, *Minimum Security Controls for Federal Information Systems*, which NIST expects to issue in 2005.

The Board currently identifies minimum controls based on the risk level assigned (high, moderate, or low) using guidance in the ISM. Information owners are to determine whether the minimum controls provide an acceptable level of security. SP 800-53, however, contains a list of controls that is much more extensive than those provided by the ISM. Going forward, the Board will need to identify the specific management, operational, and technical controls planned or in place to protect information and information systems using the guidance in SP 800-53 and FIPS 200.

Verifying Security Control Effectiveness (Certification) and Establishing Security Authorization (Accreditation)

In May 2004, NIST issued SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. SP 800-37 defines the process for performing system certifications and accreditations, to include testing and evaluation of the effectiveness of information security policies, procedures, and practices. Although the process established by SP 800-37 is effective for all systems placed into production after the publication's effective date, specific procedures for control testing and evaluation will be included in SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, which NIST expects to issue in 2005.

Currently, the information system owners complete risk certifications by verifying the existence of appropriate security controls using the list of controls contained in the ISM. Specific testing of the control's effectiveness may or may not be performed, although annual control testing is performed as part of FISMA's requirements. The information owner, generally an officer of the Board, signs off on the completed control certification and accredits the system to operate. Going forward, annual testing will remain as a FISMA requirement, but the Board will be required to complete new independent certifications (probably by someone certified to perform this function) for each system in the inventory. The certification will measure the effectiveness of the security controls associated with the information system through specific testing and evaluation. A senior Board official will then grant the authorization for the information system to process, store, or transmit information, based on the effectiveness of security controls and the acceptance of any residual risk.

ANALYSIS OF COMMENTS

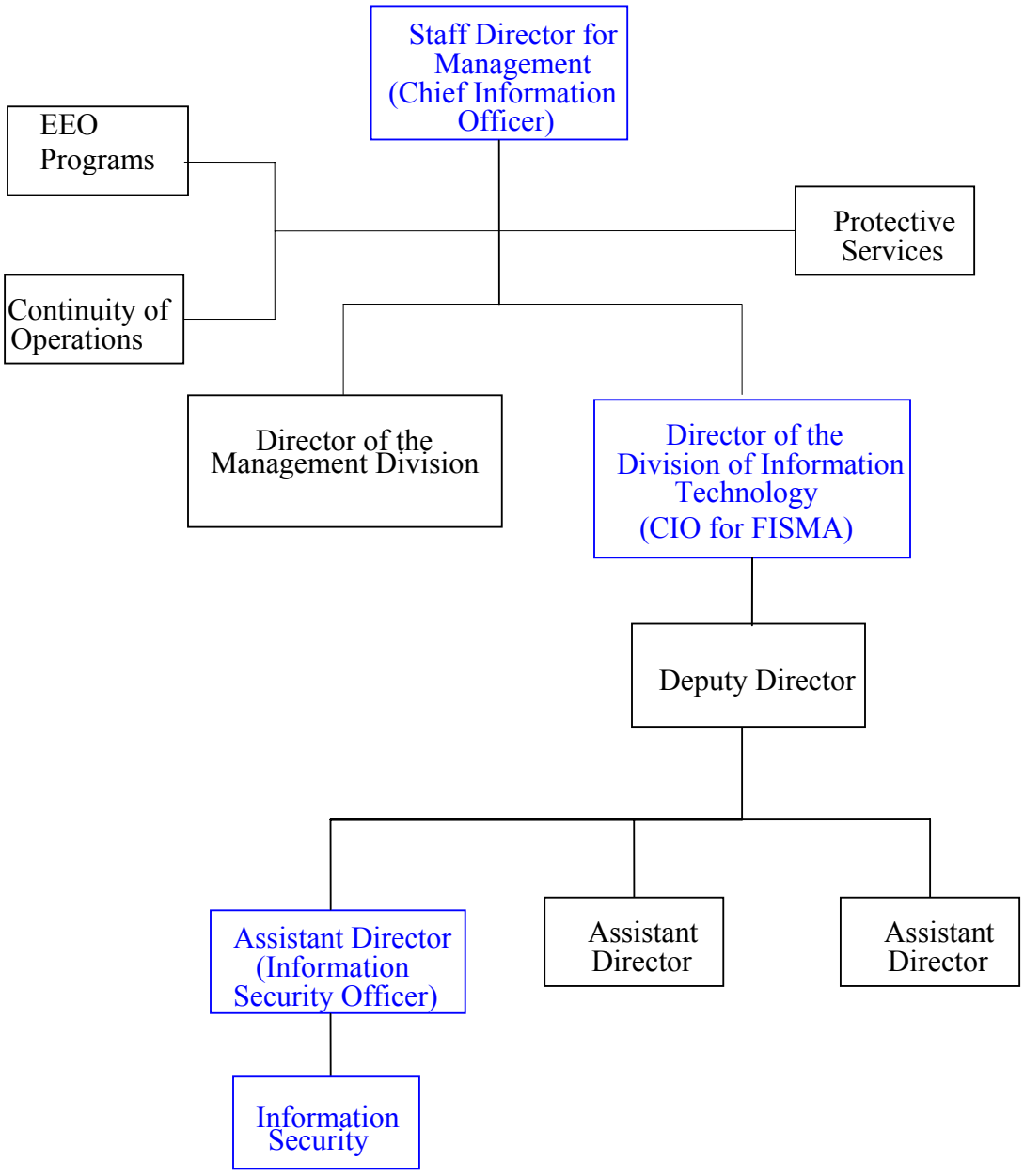
We provided our report to the director of IT, in her capacity as CIO for FISMA, for review and comment; her response is included as appendix 2. In her response, the director concurred with recommendations 1 and 3 and stated that additional guidance will be provided on the level of detail required in the POA&M and on the conduct of security control reviews. The director concurred in principle with recommendation 2, noting that any automated mechanisms implemented to measure the effectiveness of the Board's awareness training must be prioritized with other information security initiatives. The director also noted that she believes other informal feedback processes are already in place, and we will monitor these processes as part of our audit follow-up work.

The director partially concurred with recommendations 4 and 5. The director agreed that the inventory of applications and general support systems should include the identification of interfaces as required by FISMA, but she did not agree that further coordination of application reporting for FISMA and other reporting purposes was necessary. As we noted in our report, the definition of a system's criticality varies depending on the controlling law or implementing guidance. However, we are concerned that a system which has been designated as "critical" to Board operations because of legislative reporting requirements is not considered part of the Board's inventory except as part of the general support system. As the director notes in her response, FIPS 199 requires assets to be risk assessed according to standards of confidentiality, integrity, and availability. We believe that as the Board begins to apply these standards to its inventory, those applications currently designated as "other' should be similarly assessed to ensure that the controls over any system with special requirements in one of the three FIPS 199 categories are properly identified, tested, and monitored.

Regarding our recommendation concerning incident response reporting, the director agreed that the Board's reporting to FedCIRC/US-CERT should include incidents that occur at the Reserve Banks and other third-party contractors, but only when they have a material impact on Board operations. The director does not agree that expanding the Board's reporting of unsuccessful penetration attempts is useful. She believes that the information security resources required to collect and report the additional statistics are not justified, although she notes that the Board is working with FedCIRC/US-CERT in evaluating automated tools to monitor suspicious activity such as vulnerability scans or denial of service attacks. The director also expects FedCIRC/US-CERT to revise its reporting guidance regarding unsuccessful attempts. While we continue to believe that the Board needs to realign its reporting procedures with current reporting requirements, we are encouraged by its proactive efforts to identify additional methods of security incident detection. We will also monitor FedCIRC/US-CERT efforts to update collection and reporting guidance and we will review the Board's processes in light of any changes.

APPENDIXES

Appendix 1 – Board Organizational Chart for IT and Information Security



Appendix 2 – Division's Comments

September 23, 2004

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

MARIANNE M. EMERSON
DIRECTOR
DIVISION OF INFORMATION TECHNOLOGY

Mr. Barry R. Snyder, Inspector General
Federal Reserve Board
20th and Constitution Avenue, NW
Washington, DC 20551-0001

Dear Barry:

Thank you very much for the opportunity to comment on your 2004 annual review of the Board's information security program. All of the offices and divisions, especially the Division of Information Technology, have worked very diligently during 2004 to strengthen safeguards against a wide range of information security threats and to improve compliance with the de facto regulations of the Federal Information Security Act. We recognize that compliance with the changing regulatory standards will require even more resources in 2005 and 2006. My response to your specific recommendations is as follows:

1. **We recommend that the CIO enhance the process for prioritizing, tracking, and managing security performance gaps by (1) providing additional guidance on the level of detail that should be reported on POA&Ms and (2) ensuring that all security-related tasks are monitored through the Board's POA&M process.**

   We concur. Additional guidance on the level of detail required and Boardwide inclusion in the POA&M list will ensure that all security-related tasks are monitored consistently.

2. **We recommend the CIO establish a process to develop feedback on the effectiveness of the Board's security awareness and training program.**

   We concur in principle. In fact, we believe that informal feedback processes on the effectiveness of training are already in place. We can put new automation mechanisms in place to measure the effectiveness of the Board's awareness training. However, the cost of implementing these mechanisms is not trivial and therefore this recommendation must be added to the list of important information security initiatives and then funding priorities must be set.

3. **We recommend that the CIO provide guidance for conducting information security reviews that (1) includes specific requirements for control testing and (2) establishes greater consistency across all reviews.**

Appendix 2 – Division's Comments

We concur. Additional guidance will ensure that all reviewers are aware of the need for control testing and will help to achieve greater consistency.

4. We recommend that the CIO (1) expand the inventory of applications and systems to include the identification of the interfaces between each system and (2) coordinate the reporting of applications for FISMA purposes with other reporting responsibilities.

We partially concur. We agree that the inventory of applications and general support systems should include the identification of the interfaces and we have already begun to include this information. We already coordinate the reporting of applications for various responsibilities. We do not agree that the argument for further coordination of the reporting of applications for FISMA purposes with other reporting responsibilities is compelling. Federal Information Processing Standard (FIPS) publication 199 allows for information technology assets to be measured by three standards: confidentiality, integrity and availability. Each standard can be assigned a requirement level of high, medium and low. Thus an asset, such as the H.4.1 system, can have a low requirement for confidentiality and integrity and yet be have a medium availability requirement, because it is required by law to be published and thus "critical" to Board operations. It still is not a "major application" under FISMA standards. Thus, it would appear on an HSPD-7 list of mission-critical assets and not on a FISMA list of major applications.

5. We recommend the CIO expand the Board's reporting of security incidents to include all four incident priority levels as well as incidents that occur at the Reserve Banks and other third-party contractors.

We partially concur. The Board's reporting to FedCIRC/US-CERT should include incidents that occur at the Reserve Banks and other third-party contractors only when they have a material impact on Board operations. The two incident priority levels that we do not report are related to unsuccessful attempts. We do not agree that expanding the Board's reporting of unsuccessful attempts to penetrate Federal Reserve System networks is useful. A significant amount of time would need to be spent to collect and report the required statistics. Information security resources are scarce. FedCIRC/US-CERT itself recognizes that its definition of an incident is inconsistent with the definition offered by the National Institute of Standards and Technology (NIST) and that its data gathering requirement is burdensome and inefficient. We expect that FedCIRC/US-CERT will revise its guidance regarding the collection of unsuccessful attempt data and implement automated processes for collecting this type of data. Moreover, FedCIRC/US-CERT is evaluating automated tools to monitor suspicious traffic, such as vulnerability scans or denial of service attacks, against agency Internet addresses. In response, the Board has agreed to provide

Appendix 2 – Division's Comments

FedCIRC/US-CERT with its Internet-facing Internet Protocol address ranges and contact information. There is one additional aspect of incident category four that needs legal advice before being considered. That is the requirement to report monthly any misuse of resources. Reporting violations of one of the Board's permissible use policies could be a violation of an employee's right to privacy.

Sincerely,

/signed/

Marianne Emerson

Appendix 3 – Principal Contributors to this Report

Peter Sheridan, Senior EDP Auditor and Auditor-in-Charge

Richard Allen, EDP Auditor

Victor Calderon, EDP Auditor

Gerald Edwards, Auditor

Paul Sciannella, EDP Auditor

Silvia Vizcarra, Auditor

William Mitchell, Senior Program Manager